

FILED

NOV 19 2012

CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS OFFICE

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF)
THE LAW OFFICE OF LEWIS, RICE &)
FINGERSH, L.C., LOCATED AT 325 SOUTH)
HIGH STREET, BELLEVILLE, ST. CLAIR)
COUNTY, ILLINOIS)

CASE NUMBER *12-mj-3168-DWM*

FILED UNDER SEAL

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

I, John Borders being duly sworn states:

I am a Special Agent with the U.S. Department of Labor, Office of Inspector General,
and have reason to believe that on the premises known as: the entire premises of

**The Law Office Of Lewis, Rice & Fingersh, L.C., Located At 325 South High Street,
Belleville, St. Clair County, Illinois (See Attachment A)**

located in within the Southern District of Illinois there is now concealed certain property,
namely:

See the attached list entitled "Attachment B, Items to be Seized"

which constitutes evidence of the commission of a criminal offense or which is contraband, fruits
of the crime, or things otherwise criminally possessed, or which is designed or intended for use
or which is or has been used as the means of committing the following offenses: in violation of,
Title 18, United States Code, Section 641 (theft of federal unemployment funds); Title 18,
United States Code, Section 1001 (false statements); Title 18, United States Code, Section 1343
(wire fraud); Title 18, United States Code, Section 1956 (money laundering); Title 18, United
States Code, Section 1957 (money laundering); Title 26, United States Code, Sections 7201

federal unemployment funds); Title 18, United States Code, Section 1001 (false statements); Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 1956 (money laundering); Title 18, United States Code, Section 1957 (money laundering); Title 26, United States Code, Sections 7201 (attempt to evade or defeat the assessment or payment of tax); and 7206(f) (fraud and false statements, declaration under penalties of perjury). Your affiant further believes that there is supporting evidence relating to the commission of these crimes at the location further identified in this affidavit. The facts to support the issuance of a search warrant for the premises described above are as follows:

Overview:

4. Your affiant makes application for a search warrant to seize a computer belonging to **KEVIN C. WILLIAMS** that is presently in the custody of his attorney.

5. Beginning on or about July 2011, this matter has been under investigation by agents from the Internal Revenue Service, Criminal Investigations (IRS-CI). This matter was brought to the attention of IRS-CI by the civil division of IRS as a fraud referral from IRS Revenue Officer (RO) Stephanie Meents of the St. Louis, MO field office. On or about July 2012, your affiant joined the investigation.

6. At all times relevant to this search warrant application, **KEVIN C. WILLIAMS** was a Certified Public Accountant and a resident of Mt. Carmel, Illinois, who befriended a wealthy woman named [REDACTED] **WILLIAMS** helped [REDACTED] [REDACTED] manage her personal finances and he has served as the trustee for two trusts, which were established in 1991 to manage [REDACTED] family assets. **WILLIAMS** established a trusted personal relationship with [REDACTED] [REDACTED] and helped [REDACTED] manage her substantial assets because she struggled with her vision and other complications from her advanced age, which is currently 95 years of age.

12. To conceal the fact that he was misappropriating funds, **KEVIN C. WILLIAMS** supplied [REDACTED] [REDACTED] with fictitious account statements purporting to be from Lincoln Financial Group that falsely showed that [REDACTED] Spond's funds had been invested in several annuities owned by a [REDACTED] Family Trust. These fictitious account statements falsely accounted for deposits and purported to reflect increases in account values and interest payments, when in truth

and in fact, the statements were entirely fabricated to falsely verify the existence of funds which had actually been misappropriated. These phony account statements lulled [REDACTED] Spond into believing that her investments were safely invested in annuities when **WILLIAMS** had actually misapplied the funds for other purposes.

13. [REDACTED] [REDACTED] believed that her annuity investments would generate monthly interest payments. However, **WILLIAMS** had not actually invested her money as promised and there was no investment fund in place to generate the expected interest payments. Therefore, **WILLIAMS** engaged in a series of financial transactions designed to deceive [REDACTED] Spond into believing that she was receiving interest payments from investments when her money was actually being misappropriated. **WILLIAMS** misapplied money [REDACTED] Spond supplied as investment principal into the trust checking accounts that he controlled and then he purchased cashier's checks payable to Spond with money out of the same account - fraudulently passing these cashier's checks off as annuity interest payments. Thus, **WILLIAMS** simply returned small portions of [REDACTED] Spond's larger principal investments and falsely claimed those payments were annuity interest payments. **WILLIAMS** falsely verified those annuity interest payments with fictitious annuity statements purporting to originate from Lincoln Financial Group.

Investigative Findings:

14. Based on the evidence collected and presented in this affidavit, the investigative team has made the following findings and conclusions:

- a. **WILLIAMS** was employed with the law firm Rhine Ernest LLP, but was fired in March of 2011. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] WILLIAMS was subsequently fired.

b. After being fired from his job at Rhine Ernest, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c. In relation to the ongoing IRS civil activities, WILLIAMS provided some of his personal banking records to IRS RO Stephanie Meents. [REDACTED]

[REDACTED]

[REDACTED]

d. On 1/20/2011, IRS RO Stephanie Meents compared the bank records WILLIAMS provided her with original records provided directly by the bank. RO Meents observed that the records provided by WILLIAMS had been altered. The source of numerous wire transfers into WILLIAMS' account had been "whited-out" on the records WILLIAMS provided. A review of the bank records provided directly from the bank show that the "whited-out" wire transfers were from the [REDACTED] Family Trust account.

¹ WILLIAMS owes back taxes, penalties and interest of \$45,173.78 on his personal taxes for the tax years 2003, 2009 and 2010. WILLIAMS also owes excise taxes, penalties and interest of \$276,062.33 on two old businesses, Interstate Development Corp. and American Auto Centers, Inc for the tax years 2002 through 2007. On 2/18/2010 IRS attempted to levy WILLIAMS'S income from Rhine Ernest LLP.

- e. On 10/8/2010, when IRS RO Stephanie Meents questioned **WILLIAMS** about the “whited-out” deposit items, **WILLIAMS** falsely told IRS RO Stephanie Meents that the deposits were from EBay sales and tax preparation.

Federal Tax Records

15. [REDACTED]

[REDACTED]

16. The following chart illustrates the filing years, filing status, wages reported, total income and taxable income reported on the U.S. Individual Income Tax Returns:

Tax Year Ending	Filing Status	Wages Reported	Schedule C Income	Total Income	Taxable Income Reported
12/31/2008	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
12/31/2009	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
12/31/2010	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

17. [REDACTED]

18. [REDACTED]

[REDACTED]

Financial Analysis

Bank Account Analysis

19. The investigative team has reviewed and analyzed records of bank accounts controlled by **WILLIAMS** from Old National Bank, First National Bank, and Ally Bank.

Summary of Bank Records

20. According to the banking records for the [REDACTED] Family Trust accounts at Old National Bank and First National Bank, the following funds were withdrawn from the [REDACTED] Family Trust account and used for WILLIAMS' personal use:

- a. In 2008, **WILLIAMS** wrote checks to himself from the [REDACTED] Family Trust bank account in the total amount of \$176,463.50. **WILLIAMS** also paid his mortgage at CitiMortgage through the [REDACTED] Family Trust bank account in the total amount of \$19,229.22. The total amount of money **WILLIAMS** received directly or indirectly from the [REDACTED] Family Trust bank account in 2008 was \$195,692.72.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- b. In 2009, **WILLIAMS** wrote checks to himself in the total amount of \$87,594.93 and deposited \$18,600 by wire transfers into his personal account. **WILLIAMS** also paid his mortgage at CitiMortgage through the [REDACTED] Family Trust bank account in the total amount of \$14,866.38. The total amount of money **WILLIAMS** received directly or indirectly from the [REDACTED] Family Trust bank account in 2009 was \$121,061.31.

- [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

- c. In 2010, **WILLIAMS** wrote checks to himself in the total amount of \$38,383.34 and deposited \$85,392 by wire transfers into his personal account. The total amount of money **WILLIAMS** received directly or indirectly from the [REDACTED] Family Trust bank account in 2010 was \$123,775.34.

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- d. According to the bank records, E. [REDACTED] [REDACTED] transfers approximately \$25,000 from her personal account into the [REDACTED] Family Trust bank account every two to three months. **WILLIAMS** then depletes the account to a minimal balance.
- e. From 11/15/2010 to 3/23/2011, nine checks from the [REDACTED] Family Trust account were written "Pay to the order of" Old National Bank. These checks were used to purchase cashier's checks in [REDACTED] [REDACTED] name. Out of the nine checks, five of them were endorsed by **WILLIAMS** after [REDACTED] [REDACTED] endorsed the check. The cashier's checks were then deposited into [REDACTED] [REDACTED] personal account at First Bank. Based on the bank records several other checks prior to 11/15/2010 were made out to Old National Bank in similar amounts. These payments back to [REDACTED] [REDACTED] constitute examples of payments that **WILLIAMS** misrepresented as interest payments from annuities issued by Lincoln Financial Group that did not actually exist.

Detailed Analysis of Bank Records

21. According to Old National Bank records, **WILLIAMS** has signature authority on one account at this financial institution:

	Account name	Account Number	Address on Account	Date Opened
1	██████ Family Trust	*****686	██████ Mt. Carmel, IL 62863	02/22/2002

- a. According to the signature card for account number *****686, the account holder name and address is Spond Family Trust, P.O. Box 1032, Mt. Carmel, IL 62863. According to bank statements provided by Old National Bank, the account was opened on 2/22/2002 and closed on 3/24/2011.

- According to an analysis by the investigative team, from 2/6/2008 through 1/24/2011, approximately \$750,213.60 was deposited into account number *****686 by E. ██████ ██████. Also during that same time period approximately \$171,870.83 was deposited into account number *****686 from other sources. One of the other sources appears to be from **WILLIAMS** in the amount of \$77,545.05, of which \$41,100.00 comes from a brokerage account in **WILLIAMS'** name.
- An initial review, by the investigative team, of the expenditures from account number *****686, show that \$310,269.20 worth of checks were made payable to **WILLIAMS** from 1/4/2008 through 1/31/2011. In addition, checks in the amount of \$34,095.60 were made payable to CitiMortgage, in **WILLIAMS'** name, from 7/11/2008 through 6/30/2009. **WILLIAMS** also transferred \$57,124.84 to the brokerage account in **WILLIAMS'** name.

- An initial review, by the investigative team, of wire transfers made from account number *****686, show that \$110,903 was transferred to **WILLIAMS'** Ally Bank account from 11/12/2009 through 1/11/2011.

22. According to First National Bank records, **WILLIAMS** has signature authority on three separate accounts at this financial institution:

	Account name	Account Number	Address on Account	Date Opened
1	Family Life Insurance Trust	****145	██████████, Mt. Carmel, IL 62863	4/28/2011
2	Bison Development LLC/Excalibur	****787	██████████ Ladue Drive, Mt. Carmel, IL 62863	8/5/2009
3	Kevin Williams	****558	██████████ Ladue Drive, Mt. Carmel, IL 62863	8/24/2007

- a. The signature card of account ****145 shows that **WILLIAMS** is the trustee with signature authority. The signature card shows an account name and address of ██████████ Family Life Insurance Trust / ██████████, Mt. Carmel, IL 62863. According to the signature card and bank statements provided by First National Bank, the account was opened on 4/28/2011 and was closed on or around 2/22/2012.

- According to an analysis by the investigative team, from 3/24/2011 through 6/20/2011, approximately \$42,500 was deposited into account number ****145 by E. ██████████ ██████████
- An initial review, by the investigative team, of the checks drawn from account number ****145, showed that from 5/10/2011 through 6/24/2011, \$1,588.60 worth of checks were made payable to **WILLIAMS**. It also showed that \$9,020.11 worth of checks

were made payable to Excalibur Development (**WILLIAMS'** business).

b. The signature card of account number ****787 shows an account name and address of Bison Development LLC, [REDACTED] Ladue Drive, Mt. Carmel, IL 62863. The signature card also shows that **WILLIAMS** is the owner of this business and he is the only individual with signature authority on account number ****787. According to bank statements and the signature card, the account was opened first under the name Bison Development, LLC on 8/5/2009 and was charged off on 2/19/2010. The account was then reopened on 12/17/2010 and the name on the account was changed to Excalibur Development, LLC².

- According to an analysis by the investigative team, from 4/15/2011 through 7/25/2011, approximately \$14,035.30 was deposited into account number ****787 from the [REDACTED] Family Life Insurance Trust Account or E. [REDACTED] Spond's personal account at First Bank.
- An initial review, by the investigative team, of checks drawn on account number ****787, show that a majority of the checks written from the account were payable to **WILLIAMS**.

c. The signature card on account ***558 shows an account name and address of **KEVIN WILLIAMS**, [REDACTED] Ladue Drive, Mt. Carmel, IL 62863. The signature card also shows that **WILLIAMS** is the only individual with signature authority

² Bison Development, LLC filed with the state of Illinois on 7/25/2008. The active, assumed name of Bison Development, LLC is now Excalibur Development, LLC. The agent name listed for Excalibur Development, LLC is Andrew Lincoln Williams and his listed address along with the principal office is [REDACTED] Drive, Mt. Carmel, IL 62863.

on account number ****558. According to bank statements and the signature card, the account was opened on 8/24/2007 and is still currently opened.

- According to an analysis by the investigative team, from 10/22/2007 through 6/28/2011, approximately \$340,021.35 was deposited into account number ****558 from The [REDACTED] Family Trust account at Old National Bank or First National Bank.
- An initial review, by the investigative team, of the checks drawn from account number ****558, shows a majority of the checks are payable to auto companies (Plaza Motors, Expressway Ford, American Auto Centers), golf clubs and events (Victoria National, North & West Berwick, Mt. Carmel, Musselburgh Links, Ryder Cup Matches) and [REDACTED] [REDACTED]. The checks to [REDACTED] [REDACTED] occur every 3 months and are for \$1,375.

23. According to Ally Bank records, **WILLIAMS'** name is on the following account.

	Account Name	Account Number	Address on Account
1	Kevin Williams	*****031	[REDACTED] Drive, Mt. Carmel, IL 62863

- The signature card was not available for account number *****031. According to the bank statements, the name and address on the account is **KEVIN WILLIAMS**, [REDACTED] Ladue Drive, Mt. Carmel, IL 62863. According to bank statements, the account was opened prior to 12/16/2009 and is still currently open.
 - According to an analysis by the investigative team, from 2009 through 2011, approximately \$147,234.03 was transferred into

account number *****031 from the [REDACTED] Family Trust account at Old National Bank.

- An initial review, by the investigative team, of the checks drawn on account number *****031, show a majority of the checks are payable to **WILLIAMS** himself, auto companies (Landmark Chevrolet, Import Auto), golf clubs (Victoria National, West Berwick) and Citimortgage. **WILLIAMS** also made several checkcard purchases that appear personal in nature, including purchases made in the United Kingdom for golfing events (St. Andrews and other golf courses).

Unemployment Insurance Fraud

24. **WILLIAMS** filed claims for unemployment insurance with the Illinois Department of Employment Security (IDES) during various times during the years of 2007, 2008, and 2011. In order to receive unemployment insurance from IDES, a claimant must certify on a weekly basis several items to remain eligible for unemployment insurance. Most importantly the claimant must certify any weekly earnings to IDES. Depending upon the amount of earnings, the claimant's claim for unemployment insurance may be reduced or denied entirely. As indicated in the table below, **WILLIAMS** failed to report earnings when he filed claims. The amount of these earnings, if properly reported, would have resulted in complete denial of benefits.

Dates	Earnings	UI Claims During Weeks With Earnings
10/22/2007 Thru 04/08/2008	\$113,655.00	\$8,137.00
07/07/2008 Thru 10/04/2008	\$36,503.50	\$4,545.00
03/20/2011 Thru 07/02/2011	\$16,131.79	\$3,492.00
Total UI Fraud		\$16,174.00

Public Records

25. The investigative team researched and obtained **WILLIAMS'** property tax records maintained by the Wabash County Assessor's Office. The investigative team was able to determine the following: According to the 2010 Wabash County Illinois property tax records for [REDACTED] Ladue Drive, Mt. Carmel, IL 62863, **WILLIAMS** is a joint owner of the property. The other joint owner of the property is [REDACTED].

Interviews/Documents

Mt. Carmel Post Office

26. According to the application for U.S. Post Office Box Service, box number [REDACTED] has been leased by **WILLIAMS** since January of 2008. **WILLIAMS'** permanent address per the application list is [REDACTED] Ladue Drive, Mt. Carmel, IL 62863. According to records gathered by the investigative team, P.O. Box [REDACTED] was used for the address on the bank accounts for the [REDACTED] Family Trust at Old National Bank and the [REDACTED] Family Life Insurance Trust at First National Bank.

[REDACTED], First National Bank CFO Senior VP

27. The investigative team interviewed [REDACTED] on 9/9/2011 and she provided the following information:

- a. **WILLIAMS** was the Trustee for the [REDACTED] Family Trust account at First National Bank. The account is owned by [REDACTED] [REDACTED] an elderly lady (95 years old). The trust was set up in 1991 and the account was opened in April of 2011.
- b. The funds deposited into the [REDACTED] Family Trust account are personal deposits from [REDACTED] [REDACTED] personal account. A majority of the funds are then transferred

to **KEVIN C. WILLIAMS'** personal accounts at First National Bank and Ally Bank.

- c. The [REDACTED] Family Trust bank statements are being mailed to a P.O. Box 1032, Mt. Carmel, IL 62863. The bank statements for **WILLIAMS'** personal account, with address on records of [REDACTED] Ladue Drive, Mt. Carmel, IL 62863 (**WILLIAMS'** home), are emailed to **WILLIAMS**. The emailed statements confirm that **WILLIAMS** accessed evidence of the crimes from his computer. The bank statements for Excalibur Development (**WILLIAMS'** business) are being mailed to [REDACTED] Ladue Drive, Mt. Carmel, IL 62863 (**WILLIAMS'** home).

Civil IRS – RO Stephanie Meents

28. RO Stephanie Meents met **WILLIAMS** at his home ([REDACTED] Ladue Drive, Mt. Carmel, IL 62863) on 3/17/2011 to discuss his income and have **WILLIAMS** [REDACTED]

- a. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- b. [REDACTED]
[REDACTED]
[REDACTED]
- c. [REDACTED]
[REDACTED]

- d. **WILLIAMS** provided RO Stephanie Meents with his 2010 Form 1040, U.S. Individual Tax Return while she was at his house, [REDACTED] Ladue Drive, Mt. Carmel, IL 62863.

Wabash County State's Attorney

29. Wabash County State's Attorney Cassandra A. Goldman was contacted by Rhine Ernest, LLP in reference to **WILLIAMS** and his tenure at their firm. Rhine Ernest fired **WILLIAMS** once they were notified that he was not honoring the wage levy the IRS had established on his income. Rhine Ernest reviewed all documents related to **WILLIAMS**, including his computer and determined **WILLIAMS** was submitting fraudulent reimbursement expenses to Rhine Ernest. **WILLIAMS** was submitting reimbursement expenses for conferences he never attended and for software that was never downloaded on their computers.

Search Warrant #1:

30. On February 22, 2012, agents executed a federal search warrant at **WILLIAMS**' home located [REDACTED] Drive, Mt. Carmel, IL 62863. During the execution of that search warrant, agents seized records establishing that **WILLIAMS** had created fraudulent trust documents making himself the beneficiary of [REDACTED] trust. Additional investigation confirmed that **WILLIAMS** had made himself the beneficiary of [REDACTED] will and the trust beneficiary. [REDACTED] confirmed that the beneficiary changes were not authorized by her and that **WILLIAMS** was not an intended beneficiary. She successfully changed the terms of her will and the trust documents to prevent **WILLIAMS** from inheriting her money after her death.

31. Agents also recovered phony annuity account statements purporting to be from Lincoln Financial Group that **WILLIAMS** provided to [REDACTED] so that she would believe her

money was being invested in annuities with Lincoln Financial Group, when in truth and in fact **WILLIAMS** was misappropriating those funds.

32. Agents also recovered records that directed agents to additional life insurance records that date back to 1992 that show **WILLIAMS** has been continuing his scheme to defraud [REDACTED] Spond from 1992 to the present.

33. Based on **WILLIAMS'** statements, agents learned that **WILLIAMS** also had an office located at [REDACTED] College Drive, Suite [REDACTED] Mt. Carmel, Illinois. **WILLIAMS** stated that he keeps his banking records and [REDACTED] Spond's tax records at this office and offered to retrieve the documents for the agents. Agents followed **WILLIAMS** to his office located at [REDACTED] College Drive, Suite [REDACTED] Mt. Carmel, to retrieve those documents. While present inside the office, agents observed that **WILLIAMS** had a desktop computer located in his office. **WILLIAMS** also had a three in one printer, copier, scanner located in the office. However, the computer was not seized at that point because it was outside the scope of the search warrant.

34. On February 29, 2012 Special Agents with the Internal Revenue Service went back to **WILLIAMS'** office at [REDACTED] College Drive, Suite [REDACTED] Mt. Carmel, Illinois and requested consent to image **WILLIAMS'** desktop computer. **WILLIAMS** would not grant permission to image his desktop computer. Special Agents with the Internal Revenue Service put **WILLIAMS** on notice not to destroying or delete anything from his computer.

35. Shortly thereafter the United States Attorney's Office was engaged in discussions about the case with **WILLIAMS'** attorney, Frederick J. Hess. Attorney Hess is a Member of the law firm Lewis, Rice & Fingersh, L.C., whose office is located at 325 South High Street, Belleville, St. Clair County, Illinois. Hess advised the United States Attorney's Office that **WILLIAMS'**

computer that agents were seeking was now in Hess' possession at his office. Hess declined to grant consent and voluntarily provide the computer to federal authorities.

Documents on Rhine Ernst LLP's Computers

36. Members of the investigative team learned that while working at Rhine Ernst LLP, that **KEVIN WILLIAMS** performed his duties working on two computers that were owned by the firm. Agents asked an authorized representative of Rhine Ernst LLP for consent to examine the computers that **WILLIAMS** previously used for evidence. The firm consented to let SA Rusty Kiser and Cory Deters look through the two computers.

37. On August 8, 2012, Special Agents with Internal Revenue Service and Illinois Secretary of State Illinois Securities Department examined the two computers from Rhine Ernst LLP that **WILLIAMS** used while working there. The agents discovered three fraudulent Lincoln Financial Group statements addressed to Spond Family Trust, P.O. Box [REDACTED] Mt. Carmel, IL 62863, on the computer. This fact establishes that **WILLIAMS** used his computer in furtherance of the crimes enumerated in this search warrant application.

38. Based upon the foregoing, it is likely that evidence, including financial records pertaining to **WILLIAMS'** personal use of funds that were under his control as a trustee and financial advisor will also be found on the computer in the possession of attorney Frederick J. Hess, of the law firm Lewis, Rice & Fingersh, L.C., whose office is located at 325 South High Street, Belleville, St. Clair County, Illinois.

Location and Existence of Records

39. Based on information contained in an email sent to Assistant United States Attorney Norm Smith from Rick Hess (**WILLIAMS'** attorney) on September 18, 2012, and follow-up

conversations, it is known that **WILLIAMS'** computer is still located at Rick Hess's Office (325 South High Street, Belleville, IL).

40. AUSA Steven D. Weinhoeft spoke to Attorney Hess on or about November 9, 2012, and advised him that the investigative team anticipated obtaining a search warrant for **WILLIAMS'** computer. AUSA Weinhoeft asked Hess whether any grounds exist that might provide him with a basis to resist the issuance of a search warrant. Hess stated that he did not believe that any legal ground existed that would permit him to refuse to comply with a search warrant. He did, however, request that the investigators avoid inspecting the financial records belonging to **WILLIAMS's** unrelated accounting clients. Hess expressed concern that **WILLIAMS'** professional licensing requires him to protect client information from unauthorized disclosure.

Computer Searches

41. Based on your affiant's knowledge, training, experience, and information relayed to me by agents and others involved in forensic examination of computers, I know that:

- a. Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, digital, magnetic, optical or similar computer impulses or data. Hardware includes any data-processing devices (such as central processing units and self contained "laptop" or "notebook" computers or Personal Digital Assistants -- PDAs); internal and peripheral storage devices (such as fixed disks, floppy disks, external hard disks, floppy disk drives and diskettes, tape drives and optical storage devices, thumb-drives, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as

modems, cables and connections, recording equipment, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts, that can be used to restrict access to computer hardware (such as physical lock and keys).

- b. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs.
- c. Computer-related documentation consists of written, recorded, printed, or electronically-stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.
- d. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or programming codes. A password (which is a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- e. Computer hardware and computer software may be utilized to store information or data in the form of electronic, digital or magnetic coding on computer media or on media capable of being read by a computer or computer related equipment. This media includes, but is not limited to fixed hard drives and removable hard drive cartridges, laser disks, tapes, floppy disks, CD-ROMs, thumb-drives and any other media capable of storing magnetic coding.

42. Based on your affiant's knowledge, training, experience, and information relayed to me by agents and others involved in forensic examination of computers, I know that searching and seizing information from computers often requires agents to seize most or all electronic-storage devices, along with related peripherals, to be searched later by a qualified expert in a laboratory or other controlled environment for the following reasons.

- a. The volume of evidence. Computer storage devices (like hard disks, diskettes, thumb-drives, tapes, laser disks) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
- b. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed,

password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

- c. Searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer’s input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the computer’s data in a laboratory or other controlled environment. This is true because of the following:

- The peripheral devices which allow the users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many systems storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the computer as it now operates in order to accurately retrieve the evidence.
- In addition, the analyst needs the relevant system software (operating systems, interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals, or other documentation and data security devices.


43. In light of the concerns outlined above, your affiant hereby requests the Court’s permission to seize **WILLIAMS’** computer hardware and associated peripherals that are

believed to contain some or all of the evidence described in the warrant and to conduct an offsite search of the hardware for the evidence described herein.

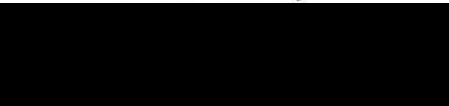
Affiant's Conclusion

44. Based on the forgoing, your affiant alleges there is probable cause to believe that on the premises described herein, there is presently concealed those items set forth in Attachment B, which constitutes evidence of violations of Title 18, United States Code, Section 641 (theft of federal unemployment funds); Title 18, United States Code, Section 1001 (false statements); Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 1956 (money laundering); Title 18, United States Code, Section 1957 (money laundering); Title 26, United States Code, Sections 7201 (attempt to evade or defeat the assessment or payment of tax); and 7206(1) (fraud and false statements, declaration under penalties of perjury).

FURTHER AFFIANT SAYETH NAUGHT



JOHN BORDERS
US Dept. of Labor

STEPHEN R. WIGGINTON
United States Attorney


STEVEN D. WEINHOFET
Assistant United States Attorney

State of Illinois)
) SS.
County of Saint Clair)

Sworn to before me, and subscribed in my presence on the 17th day of November, 2012, at East Saint Louis, Illinois


Honorable Donald G. Wilkerson
United States Magistrate Judge

Attachment A

A DESKTOP COMPUTER OWNED BY KEVIN C. WILLIAMS LOCATED WITHIN
THE PREMISES OF THE LAW FIRM OF LEWIS, RICE & FINGERSH, L.C., 325
SOUTH, HIGH STREET, BELLEVILLE, ST. CLAIR COUNTY, ILLINOIS,
DESCRIBED AS A TWO STORY SQUARE OFFICE BUILDING COVERED IN BRICK
ON ALL FOUR SIDES.

Attachment B
Items to be Seized

Property which constitutes evidence of the commission of a criminal offense or which is contraband, fruits of the crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of committing an offense impacting the 1992 through 2012: of violations of Title 18, United States Code, Section 641 (theft of federal unemployment funds); Title 18, United States Code, Section 1001 (false statements); Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 1956 (money laundering); Title 18, United States Code, Section 1957 (money laundering); Title 26, United States Code, Sections 7201 (attempt to evade or defeat the assessment or payment of tax); and 7206(1) (fraud and false statements, declaration under penalties of perjury).

A. KEVIN WILLIAMS COMPUTER:

1. Trust records, to include trust creation documents, tax returns (including drafts and unfiled copies), bank statements, account applications, signature cards, deposit items, cancelled checks, withdrawal items, cash withdrawals, checks to cash, wire transfers, cashier's checks, money orders, traveler's checks, bank checks, official checks, cash advance checks, passbooks, records of safety deposit boxes and keys, monthly statements, investment accounts, foreign bank accounts, and the transfer, expenditure, and obtaining of money, credit card and debit card statements, brokerage account records, stocks and bonds, real estate, and commodities, loan applications and documents, lists of assets, monthly payment slips, receipts, notifications of payments received, mortgage applications and documents, credit checks, and amortization statements, credit card statements, credit card applications, trustee documents, beneficiary documents, grantor documents;

2. Business accounting records, to include accounting ledgers, payment ledgers, general ledgers, ledgers of cash receipts and disbursements, accounts payable, accounts receivable, financial statements, notes, payroll disbursements, payroll federal tax withheld, payroll Social Security tax withheld, payroll Medicare tax withheld, all tax related information, and all other summaries and compilations of financial information;

3. Business and personal financial institution records, to include account applications, signature cards, deposit items, cancelled checks, withdrawal items, cash withdrawals, checks to cash, wire transfers, cashier's checks, money orders, traveler's checks, bank checks, official checks, cash advance checks, passbooks, records of safety deposit boxes and keys, monthly statements, investment accounts, foreign bank accounts, and the transfer, expenditure, and obtaining of money, credit card and debit card statements, brokerage account records, stocks and bonds, real estate, and commodities;

4. Business and personal loan records, to include loan applications and documents, tax returns, lists of assets, monthly payment slips, receipts, notifications of payments received, mortgage applications and documents, credit checks, and amortization statements;

5. All financial and investment records related to financial transactions, assets, or investments, including the following: credit card statements, debit card statements, financial institution records, mortgage documents, mortgage applications, credit checks, loan documents, loan applications, brokerage records, stocks, bonds, real estate and commodities;

6. Books, records, receipts, bank statements and records, money drafts, letters of credit, money orders and cashier's checks, receipts, passbooks, bank checks and other items evidencing the obtaining, transfer and/or concealment of assets and the obtaining, secreting, transfer, concealment and/or expenditure of money;

7. Business and personal IRS forms and related documents, manuals, correspondence, and booklets, to include originals and copies of U.S. Individual Income Tax Returns and/or state tax returns and related documents;

8. Business incorporation and licensing applications or documents;

9. Telephone records, cellular phone, and other devices that save phone and/or address books, names, addresses, text messages, and phone numbers, emails and electronic data;

10. Documents, tickets, notes, receipts and other items relating to domestic and international travel; All of the foregoing items of evidence described in paragraphs 1-11 above, in whatever form and by whatever means such items may have been created or stored, including any hand-made form, any photographic form or any electrical, electronic, digital or magnetic form, such as any information on an electronic, digital or magnetic storage device like a floppy diskette, hard disk, backup media, CD-ROM, thumb-drive, optical disc, electronic dialer, electronic notebook, as well as printouts or readouts from any digital or magnetic storage device;

11. Computer hardware, including data-processing devices (such as central processing units, desktop computers, self-contained "laptop" or "notebook" computers,); internal and peripheral storage devices (such as fixed disks, floppy disks, external hard disks, floppy disk drives and diskettes, tape drives and optical storage devices, thumb-drives, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts, that can be used to restrict access to computer hardware (such as physical lock and keys);

12. Computer software, including programs to run operating systems, applications, utilities, compilers, interpreters, video, web browsers, and communications programs;

13. All computer passwords and data security devices, including encryption devices, chips and circuit boards.